Sumário

Generalidades 2

Antes da instalação 3

Instalação 7

G Data MailSecurity MailGateway 9

G Data MailSecurity Administrator 11

Área do programa do administrador 13

Barra de menu do Administrator 26

Acordo de licença 43

Generalidades

A proteção segura contra vírus e spam para sua correspondência de e-mail. O *G Data MailSecurity* trabalha como ***Gateway*** independente de seu ***servidor de e-mail***; por essa razão, ele é o software de servidor de e-mails preferencial sob o Windows, assim como combinável com Linux, e protege sua correspondência baseada em SMTP ou POP3, de forma segura contra vírus, spam, phishing e outras pragas - antes que alcancem seu servidor.

BT1 - G Data MailSecurity Administrator
MailSecurity
Opções
Atualização
Filtro de spam
Ajuda
Informações
Status
Indicação do status atual do G Data MailSecurity. Com um clique duplo (botão esquerdo do mouse) é possível editar as funções individuais.
Processamento de e-mails de entr... SMTP
Verificação de vírus em e-mails de... Ativo
Processamento de e-mails de saída Ativo
Verificação de vírus em e-mails de... Ativo
OutbreakShield Ativo
Atualizações automáticas G Data AntiVirus Client
Data das assinaturas de vírus 23/07/2010
Filtro de spam Ativo
Spam-OutbreakShield Ativo
Quanto mais atual for a assinatura de vírus, mais segura é a sua proteção antivírus. Você deve atualizar as assinaturas de vírus com a maior frequência possível.
Editar...
Status
Filtro
Filas de espera
Atividade
Vírus detectado

Desejamos um trabalho bem-sucedido com o *G Data MailSecurity*!

Sua equipe *G Data*

G Data PremiumHotline

A instalação e utilização do *G Data Software* é normalmente intuitiva e descomplicada. Se ocorrer um problema em algum momento, basta entrar em contato com o***Suporte técnico G Data*** através da Internet.

www.gdatasoftware.com.br

Antes da instalação

O *G Data MailSecurity* é o pacote de software para a proteção completa de sua comunicação por e-mail. Ele abrange:

- ***G Data MailSecurity MailGateway***: O *MailGateway* é uma proteção de vírus High End para sua correspondência de e-mail e tranca, assim, o principal caminho de propagação de vírus de forma eficiente e segura. Ele trabalha como Gateway independente de seu servidor de e-mail e, portanto, é combinável a softwares de servidor de e-mail sob Windows ou Linux.
- ***G Data MailSecurity Administrator***: Software de controle para o MailGateway.

O programa é um MailGateway para SMTP e POP3 com proteção antivírus integrada.

- ***SMTP***: E-mails de entrada não são mais enviados ao servidor de e-mail, mas ao *G Data MailSecurity MailGateway*. Após a verificação de vírus, ele são enviados, de lá, ao servidor de e-mail. O *G Data MailSecurity* pode também, naturalmente, verificar os e-mails de saída. Para isso, o servidor de e-mail é configurado de tal forma que ele não envia os e-mails diretamente, mas os encaminha primeiro ao *G Data MailSecurity*. Só então é que o programa se ocupa do resto do processamento.
- ***POP3***: O *G Data MailSecurity* também pode ser utilizado quando você captura seus e-mails via POP3. O *G Data MailSecurity* pega, como substituto, os e-mails para o programa solicitante, verifica-os quanto a virus e os encaminha ao programa.

Naturalmente, antes da instalação, você deve se preocupar onde instalar, na rede, o *G Data MailSecurity*. Enquanto o *software Administrator do G Data MailSecurity* pode ser utilizado de qualquer ponto da rede, a instalação do MailGateways precisa de algumas pré-considerações Em geral, o MailGateway deve se encontrar diretamente atrás do firewall de sua rede (se existente), ou seja, o fluxo de dados SMTP/POP3 da Internet é encaminhado através do ***Firewall*** diretamente para o MailGateway e de lá novamente encaminhado.

? Observe que, eventualmente, será necessário alterar suas ***configurações de firewall*** (endereço IP e/ou porta) para que o tráfego de e-mail seja feito através do *G Data MailSecurity MailGateway*.

Em princípio, o *G Data MailSecurity MailGateway* pode ser instalado em um computador próprio que então funcione para toda a rede como MailGateway, mas é possível utilizar o *G Data MailSecurity* no computador que funciona simultaneamente como servidor de e-mail. Aqui deve-se observar que uma instalação completa em um único computador pode levar a retardos em grandes volumes de e-mails, porque tanto a administração da comunicação de e-mail permanente como as análises de vírus iminentes são processos que utilizam bastante o computador.

Instalação do MailGateway no servidor de e-mail (SMTP)

Quando o seu ***servidor de SMTP*** também permite a alteração do número da porta, você pode instalar o *G Data MailSecurity* no mesmo computador que o seu servidor de SMTP. Neste caso, atribua, ao servidor de e-mail original, um novo número de porta (p.ex., 7100 ou superior). O *MailGateway* continuará a utilizar a ***Porta 25*** para o processamento dos e-mails de entrada.

? Se o *G Data MailSecurity* for instalado no mesmo computador que o ***Microsoft Exchange 5.5***, o *setup do G Data MailSecurity Setup* pode mudar automaticamente a porta para e-mails de entrada.

Para isso, o registro do SMTP é alterado no arquivo ***\winnt\system32\drivers\etc\services*** e o serviço de e-mail da Internet do Microsoft Exchange é reiniciado.

Exemplo:

Configuração do servidor de e-mail

- Porta para e-mails de entrada: 7100 (exemplo)
- Transmissão da mensagem: Encaminhar todas as mensagens ao host: 127.0.0.1

Configuração do G Data MailSecurity MailGateway (De entrada (SMTP))

- Porta na qual os e-mails entram: 25
- Utilizar DNS para envio de e-mails: DESATIVADO
- Encaminhar e-mails para este servidor de SMTP: 127.0.0.1
- Porta: 7100 (exemplo)

Configuração do G Data MailSecurity MailGateway (De saída (SMTP))

- Processar e-mails de saída: ATIVADO
- Endereços IP do servidor que podem enviar e-mails: 127.0.0.1; <IP do servidor de e-mail>
- Utilizar DNS para envio de e-mails: ATIVADO

Designações

- <IP do servidor de e-mail> = endereço IP do computador onde o servidor de e-mail está instalado:
- <IP G Data MailSecurity> = Endereço IP do computador onde o G Data MailSecurity MailGateway está instalado.

Instalação do MailGateway em computadores separados (SMTP)

Aqui os e-mails de entrada devem ser enviados ao *G Data MailSecurity MailGateway* (não ao servidor). Isso pode ser realizado através de diferentes métodos:

a) adaptar o ***registro MX*** no ***registro DNS***

b) definir o desvio no ***Firewall*** (caso existente)

c) alterar o ***Endereço IP*** do servidor de e-mail e atribuir ao computador com o *G Data MailSecurity MailGateway* o endereço IP original do servidor de e-mail

? ***Configuração do servidor de e-mail***

- Porta para e-mails de entrada: 25
- Transmissão da mensagem: Encaminhar todas as mensagens ao host: <IP do G Data MailSecurity>

Configuração do G Data MailSecurity MailGateway (De entrada (SMTP))

- Porta na qual os e-mails entram: 25
- Utilizar DNS para envio de e-mails: DESATIVADO
- Encaminhar e-mails para este servidor de SMTP: <IP do servidor de e-mail>
- Porta: 25

Configuração do G Data MailSecurity MailGateway (De saída (SMTP))

- Processar e-mails de saída: ATIVADO
- Endereços IP do servidor que podem enviar e-mails: <IP do servidor de e-mail>
- Utilizar DNS para envio de e-mails: ATIVADO

Designações

- <IP do servidor de e-mail> = endereço IP do computador onde o servidor de e-mail está instalado:
- <IP G Data MailSecurity> = Endereço IP do computador onde o G Data MailSecurity MailGateway está instalado.

Requisitos do sistema

Para utilização do *G Data MailSecurity*, é preciso avaliar o seguinte espaço de armazenamento em disco:

- Pré-requisitos para a utilização do *G Data MailSecurity Administrator*: Pentium PC com 32 MB RAM. Sistemas operacionais possíveis: Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2.
- Pré-requisitos para o *G Data MailSecurity MailGateway*: Pentium PC com 256 MB RAM, unidade de CD-ROM, acesso à Internet. Sistemas operacionais possíveis: Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2.

? O *G Data MailSecurity* também pode ser executado em sistemas operacionais Windows com 64 bits.

Instalação

Feche todos os outros programas antes de começar a instalação do *G Data MailSecurity*. Se forem abertos programas que acessem os dados necessários para a instalação do *G Data MailSecurity*, podem ocorrer erros de funcionamento ou uma interrupção. Observe também se, para uma instalação, existe espaço suficiente no disco rígido em seu sistema. Se durante a instalação o espaço livre no disco não for suficiente, o programa de instalação do *G Data MailSecurity* informará isso.

A instalação do *G Data MailSecurity* é extremamente fácil. Basta iniciar o Windows e colocar o *CD-ROM do G Data MailSecurity* na sua unidade de CD-ROM. Uma janela de instalação abre automaticamente e oferece as seguintes opções:

- **Instalar**: Através dessa opção, você inicia a instalação do *G Data MailSecurity* em seu computador.
- **Procurar**: Através do Windows Explorer, você poderá visualizar os diretórios de CD-ROM do *CD-ROM do G Data MailSecurity*.
- **Cancelar**: Através desse registro você pode fechar a tela de inicialização automática sem executar uma ação.

? Se não tiver ativado o ***recurso de inicialização automática de sua unidade de CD-ROM*** , o *G Data MailSecurity* não pode iniciar automaticamente o processo de instalação. Assim, clique no ***menu Iniciar*** do Windows, em ***Executar***, na janela que aparece, digite ***e:\setup.exe*** e clique em ***OK***. Dessa forma, a tela de inicialização também é aberta para a*instalação do G Data MailSecurity*. O registro ***e:*** indica a letra da unidade de sua unidade de CD-ROM. Se tiver registrado a sua unidade de CD-ROM em uma outra letra, insira, ao invés de ***e:*** a letra da unidade correspondente.

Agora basta seguir os passos individuais do assistente de instalação e instalar, através do botão **G Data MailSecurity**, o MailGateway no computador em que deseja utilizar para isso. Na melhor das hipóteses, esse deverá ser um computador especialmente separado para isso, mas também o próprio computador do servidor de e-mail ou um outro computador que possa assumir na rede tarefas administrativas. Em relação a isso, observe os ***pré-requisitos mínimos*** necessários para a operação do MailGateway.

? Através da etapa de instalação **Estatística de E-Mail**, você pode instalar junto uma avaliação estatística do tráfego de e-mail no servidor de e-mail. Ao utilizar essa opção, em **Opções** no menu do administrador, você encontrará uma guia adicional chamada **Banco de dados**.

G Data MailSecurity MailGateway

Após a conclusão da instalação, o *software MailGateway* estará disponível. Além do software em si, que é executado em segundo plano, o ***Administrador*** é automaticamente instalado, através do qual você tem acesso completo às funções e opções do MailGateway. Esse Administrator, você encontra em uma instalação padrão em ***Iniciar > Programas > G Data MailSecurity > G Data MailSecurity***. As possibilidades de configuração e influenciamento NÃO SERIAM INFLUÊNCIAS?? disponíveis através do Administrator são explicadas detelhadamente nos capítulos a seguir.

? O MailGateway também pode ser mantido através de qualquer outro computador que atenda aos pré-requisitos para a ferramenta do *G Data MailSecurity Administrator*. Quando desejar controlar o MailGateway também através de um outro computador na rede, basta instalar lá o Administrator sem o software MailGateway em si. Para isso, basta reiniciar o setup e selecionar o botão ***G Data MailSecurity Administrator*** aus.

? Ao finalizar o software Administrator, você não fecha o MailGateway. Esse permanece ativo em segundo plano e controla os processos que foram definidos por você.

O recebimento e envio de ***E-Mails*** é normalmente feito através dos dois protocolos ***SMTP*** e ***POP3***. Neste processo, o SMTP (= Simple Mail Transfer Protocol) serve para enviar e-mails aos destinatários desejados, enquanto o POP3, (= Post Office Protocol 3) como protocolo superior é utilizado para depositar os e-mails de entrada em uma *caixa postal* especial, à qual somente o destinatário especial tem acesso através de uma senha. Dependendo de como a sua rede é estruturada, o *G Data MailSecurity* só pode acessar diferentes pontos de nós para verificar os e-mails de entrada quanto à infecção por vírus:

- Quando você utiliza um ***servidor de SMTP*** na rede, o *G Data MailSecurity* pode verificar os e-mails de entrada, já antes de chegarem ao servidor de e-mail. Para isso, a função **verificação de e-mails de entrada (SMTP)** na ***Área de status*** está disponível.
- Quando você recebe seus e-mails, p.ex., através de um servidor externo diretamente como ***e-mails POP3*** (p.ex., através de uma ***conta POP3 reunida***), o *G Data MailSecurity* pode também acessá-la para verificar os e-mails POP3 antes de serem abertos pelo destinatário. Para isso, a função **verificação de e-mails de entrada (POP3)** na ***Área de status*** está disponível.

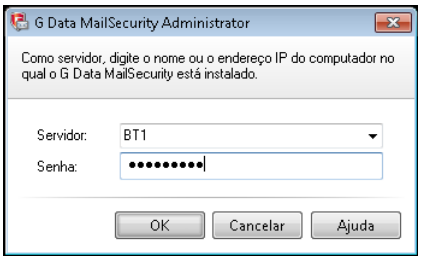
Naturalmente o *G Data MailSecurity* também pode verificar todos os seus e-mails de saída antes do envio ao destinatário, quanto à infecções de vírus. Como para o envio de e-mails somente o registro SMTP é utilizado, não existe aqui logicamente nenhuma variação de POP3. Para isso, a função **verificação de e-mails de saída (SMTP)** na ***Área de status*** está disponível.

G Data MailSecurity Administrator

O *G Data MailSecurity Administrator* é o software de controle para o *G Data MailSecurity MailGateway* que, controlado pelo administrador centralmente, protege todo o tráfego de e-mail baseado em POP3 e SMTP e a sua rede. O ***Administrator*** pode ser iniciado protegido por senha, a partir de qualquer computador com Windows. Como tarefas controladas remotamente, todas as possíveis alterações de configuração no verificador de vírus e atualizações de assinaturas são possíveis.

Primeira inicialização do programa (atribuição de senha)

A ferramenta ***Administrator*** pode ser aberta para controle do ManagementServers com um clique no registro ***G Data MailSecurity Administrator*** no grupo de programas ***Iniciar > (Todos os) Programas > G Data MailSecurity Administrator*** no menu Iniciar. Na inicialização do Administrator, você será perguntado pelo servidor e senha.



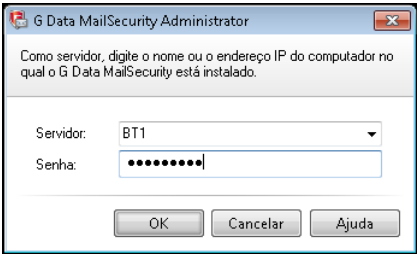
No campo **Servidor**, insira o nome do computador ou o endereço IP no qual o MailGateway foi instalado. Como ainda não atribuiu nenhuma **Senha**, clique no botão **OK** sem inserir uma senha. Uma janela para entrada da senha será aberta, na qual, em **Senha nova:**, você poderá atribuir uma nova senha para o *G Data MailSecurity Administrator*.

Confirme a senha inserida através da redigitação em **Confirmar senha nova** e clique, depois, em **OK**.

? A senha pode novamente ser atribuída a qualquer momento na área **Opções** na guia **Avançado** com um clique no botão **Alterar senha**.

Outras inicializações do programa (senha de acesso)

A ferramenta Administrator pode ser aberta para controle do MailGateway com um clique no registro ***G Data MailSecurity Administrator*** no grupo de programas ***Iniciar > (Todos os) Programas > G Data MailSecurity*** no menu Iniciar. Na inicialização do Administrator, você será perguntado pelo servidor e senha.



No campo **Servidor**, insira o nome do computador ou o endereço IP no qual o MailGateway foi instalado.

Área do programa do administrador

A utilização do *G Data MailSecurity* é, em princípio, intuitiva e estruturada de forma clara. Com auxílio de diferentes guias que podem ser selecionadas por meio dos ícones exibidos à esquerda no *G Data MailSecurity Administrator*, você alterna para a respetiva área do programa e lá pode executar ações, predefinir configurações ou verificar processos. Estão disponíveis as seguintes áreas do programa:

Status

Filtro

Filas de espera

Atividade

Vírus detectado

Além disso, você encontra várias funções e possibilidades de configuração na barra de menu superior da interface do programa.

Opções: aqui você pode alterar as configurações básicas para funcionamento do *G Data MailSecurity* e adaptá-las às necessidades individuais.

Filtro de spam: através do Filtro de spam, você tem amplas possibilidades de configuração para bloquear, de forma eficaz, os e-mails com conteúdo ou remetentes indesejados (p.ex., remetentes de e-mail em massa).

Atualizar: na área Atualização na Internet, é possível fazer configurações básicas para download automático das assinaturas de vírus atuais da Internet. A programação temporal para esses downloads pode ser adaptada às necessidades individuais e, além disso, executar atualizações dos arquivos de programa do *G Data MailSecurity*.

Ajuda: Aqui você abre a ajuda on-line para o produto.

Informações: Aqui você obtém informações sobre a versão do programa.

Status

Na área de status do Administrator, você obtém informações básicas sobre a situação atual de seu sistema e do MailGateway.

BT1 - G Data MailSecurity Administrator
MailSecurity
Opções
Atualização
Filtro de spam
Ajuda
Informações
Status
Indicação do status atual do G Data MailSecurity. Com um clique duplo (botão esquerdo do mouse) é possível editar as funções individuais.
Processamento de e-mails de entr... SMTP
Verificação de vírus em e-mails de... Ativo
Processamento de e-mails de saída Ativo
Verificação de vírus em e-mails de... Ativo
OutbreakShield Ativo
Atualizações automáticas G Data AntiVirus Client
Data das assinaturas de vírus 23/07/2010
Filtro de spam Ativo
Spam-OutbreakShield Ativo
Quanto mais atual for a assinatura de vírus, mais segura é a sua proteção antivírus. Você deve atualizar as assinaturas de vírus com a maior freqüência possível.
Editar...
Status
Filtro
Filas de espera
Atividade
Vírus detectado

Essas podem ser encontradas à direita do respetivo registro como informações em texto, número ou data.

Enquanto o seu *G Data MailSecurity* estiver idealmente configurado para a proteção contra vírus de computador você encontrará, à esquerda dos registros aqui relacionados, um sinal verde.

Se um componente não estiver configurado adequadamente (p. ex., a assinaturas de vírus desatualizadas, verificação de vírus desativada), um sinal de aviso indicará isso.

Com um clique duplo no respectivo registro (ou, através da seleção do registro e um clique no botão **Editar**) você pode tomar providências diretamente aqui ou alternar para a respectiva área do programa. Assim que tiver otimizado as configurações de um componente com o ícone de atenção, ele torna-se novamente para o sinal verde na área de status. Estão disponíveis os seguintes registros:

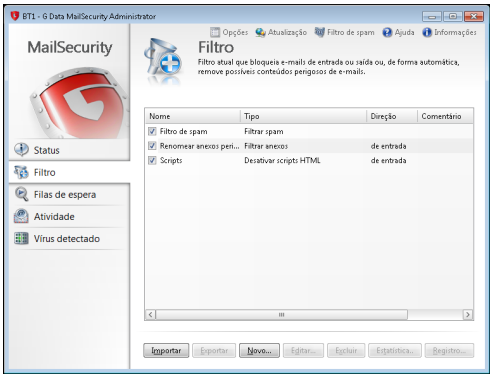
- **Processamento de e-mails de entrada**: O processamento de e-mails de entrada faz com que eles, antes do redirecionamento ao destinatário, sejam verificados pelo MailGateway. Um clique duplo nesse registro o direcionará para a respetiva janela de configuração (barra de menu: ***Opções > De entrada (SMTP)***) e poderá adaptar o processamento de e-mails de entrada às necessidades individuais.
- **Verificação de vírus em e-mails de entrada**: A verificação de e-mails de entrada impede que arquivos infectados cheguem a sua rede. Um clique duplo nesse registro o direcionará para a respetiva janela de configuração (barra de menu: ***Opções > Verificação de vírus***) e poderá adaptar a verificação de e-mails de entrada às necessidades individuais.
- **Processamento de e-mails de saída**: O processamento de e-mails de saída faz com que os e-mails, antes do redirecionamento ao destinatário, sejam verificados pelo MailGateway. Um clique duplo nesse registro o direcionará para a respetiva janela de configuração (barra de menu: ***Opções > De saída (SMTP)***) e poderá adaptar o processamento de e-mails de saída às necessidades individuais.
- **Verificação de vírus em e-mails de saída**: A verificação de e-mails de saída evita que arquivos infectados sejam enviados da sua rede. Um clique duplo nesse registro o direcionará para a respetiva janela de configuração (barra de menu: ***Opções > Verificação de vírus***) e poderá adaptar a verificação de e-mails de saída às necessidades individuais.
- **OutbreakShield**: Com a ***OutbreakShield***, é possível o reconhecimento e combate de pragas em e-mails em massa, antes que as assinaturas atualizadas estejam disponíveis. A OutbreakShield consulta, na Internet, sobre acúmulos especiais de e-mails suspeitos e fecha, quase em tempo real, a brecha que existe entre o começo de um e-mail em massa e seu combate através de assinaturas de vírus adaptadas especialmente.
- **Atualizações automáticas**: Naturalmente as assinaturas de vírus podem ser atualizadas automaticamente. A opção para ***atualizações*** automáticas deverá estar, em geral, ativada. Um clique duplo nesse registro o direcionará para a respetiva janela de configuração (barra de menu: ***Atualização na Internet***) e poderá adaptar a frequência das atualizações às necessidades individuais.
- **Data das assinaturas de vírus**: Quanto mais atuais forem as assinaturas de vírus, mais segura é sua proteção antivírus. As ***Assinaturas de vírus*** devem ser atualizadas com a maior frequência possível para automatizar, ao máximo, esse processo. Um clique duplo nesse registro o direcionará para a respetiva janela de configuração (barra de menu: ***Atualização na Internet***) e poderá executar diretamente uma atualização na Internet (independente de programações existentes).

- **Filtro de spam**: Através do ***Filtro de spam*** você tem amplas possibilidades de configuração para bloquear, de forma eficaz, os e-mails com conteúdo ou remetentes indesejados (p.ex., remetentes de e-mail em massa).
- **Spam-OutbreakShield**: Com a ***Spam-OutbreakShield***, e-mails em massa podem ser rápido e seguramente reconhecidos e combatidos,. A Spam-OutbreakShield questiona, antes da abertura de e-mails através da Internet, acúmulos estranhos de e-mails suspeitos e não os deixa nem chegar à caixa postal do destinatário.

? Quando antes da instalação a opção **estatística de e-mail** for ativada, através do botão **Estatística**, é possível ter acesso à avaliação estatística de seu tráfego de e-mail ou surgimento de spams. A configuração da estatística é feita no menu **Opções** do administrador, na guia chamada **Banco de dados**.

Filtro

Na área de filtro, você pode utilizar confortavelmente filtros que bloqueiam e-mails de entrada e saída ou remover automaticamente conteúdo perigoso de e-mails. Os respetivos filtros criados são exibidos na lista na área de filtros e podem ser ativados ou desativados conforme desejado, na marcação à esquerda do respetivo registro.



Quando houver uma marcação no campo da marcação, o respetivo filtro está ativo. Quando não houver uma marcação no campo, o respectivo filtro não está ativo.

- **Importar**: Os filtros individuais podem ser salvos também como arquivos XML, com suas configurações especiais e, eventualmente, serem usados novamente ou em outros computadores.

- **Exportar**: Os filtros individuais podem ser salvos também como arquivos XML, com suas configurações especiais e, eventualmente, serem usados novamente ou em outros computadores. Para exportar diversos filtros, selecione-os com o mouse e mantenha a tecla ***Ctrl*** pressionada.
- **Novo**: Através do botão **Novo**, é possível criar novas regras de filtragem. Quando um novo filtro é criado, uma janela de opções é aberta, onde é possível definir o tipo de filtro básico. Todos os outros dados para o filtro a ser criado podem ser inseridos em uma janela assistente apropriada. Dessa forma, você cria confortavelmente filtros contra todos os tipos de perigo.
- **Editar**: Através do botão **editar**, você pode editar filtros existentes.
- **Excluir**: Para excluir o filtro permanentemente, selecione-o com um clique do mouse e utilize em seguida o botão **Excluir**.
- **Estatística**: Para cada filtro, é possível abrir informações estatísticas.
- **Registro**: Para o ***filtro de spam***, existe um registro com uma lista na qual os e-mails classificados como spam são listados. Do registro, é possível saber quais os critérios para classificação como spam foram os responsáveis (Valores do índice de spam). Aqui, se necessário, no caso de uma classificação errônea de um e-mail como spam, você pode informar ao servidor OutbreakShield- online que ocorreu uma deteção falsa (*Falso positivo*). O e-mail será novamente verificado pelo OutbreakShield e, caso realmente tenha sido erroneamente classificado como spam, será classificado como inofensivo. ***Atenção***: Aqui só uma soma de verificação é transmitida e não o conteúdo desse e-mail.

? Naturalmente a sua rede independente também de regras de filtragem individuais protegida contra infecções de vírus, porque o *G Data MailSecurity* verifica constantemente, em segundo plano, os e-mails de entrada e saída. As regras de filtragem servem mais para proteger suas contas de e-mail contra e-mails indesejados e scripts perigosos, além de minimizar as manadas de vírus potenciais, já antes da detecção de vírus em si, pelo *G Data MailSecurity*.

? ***Funções gerais dos filtros***
Em geral, você pode inserir, para todos os tipos de filtro, em **Nome**, um nome representativo para o respetivo filtro a ser exibido na lista da área de filtros e, em **Comentário**, inserir comentários internos e avisos sobre ele. Em **Direção**, você pode definir generalizadamente se uma regra de filtragem deve valer apenas para ***e-mails de entrada***, apenas para ***e-mails de saída*** ou em ambas as direções.

? ***Reação***
Na seção **Reação**, você pode definir como deverá ser procedido com os e-mails, assim que atenderem aos critérios de pesquisa, ou seja, que foram definidos como e-mails spam.

Para isso, é possível formular o texto para as funções**Notificar remetente** e **Enviar mensagem às seguintes pessoas** individualmente.

Para isso, basta clicar no botão à direita de cada respetiva reação. Para isso, também é possível utilizar espaços reservados que aplicam respetivamente os dados para o e-mail rejeitado no texto da notificação. Os seguintes **espaços reservados** existem à disposição no texto livremente definível para o **Assunto** e **Texto do e-mail** (definido por um sinal de percentual seguido por uma letra minúscula):

- %s ***Remetente***
- %r ***Destinatário***
- %c ***Cc***
- %d ***Data***
- %u ***Assunto***
- %h ***Cabeçalho***
- %i ***IP do remetente***

Os diferentes tipos de filtro são descritos de forma detalhada nos próximos parágrafos:

Filtrar confirmação de leitura

Esse filtro exclui solicitações de confirmação de leitura. Aqui se trata de um e-mail de resposta enviado automaticamente, assim que o destinatário tenha lido um e-mail com confirmação de leitura.

Desativar scripts HTML

Esse filtro desativa scripts na parte HTML de um e-mail. Scripts que possam ter um sentido em uma página da Internet, são bastante perturbadores quando estão anexados em um e-mail em HTML. Em alguns casos, os scripts HTML são utilizados ativamente para infectar arquivos, onde os scripts têm a possibilidade de não se propagar apenas com a abertura de um anexo infectado, mas, por si só, podem ter efeito já na ***pré-visualização*** de um e-mail.

Desativar referências externas

Muitos boletins informativos e informações de produto no ***formato de e-mail HTML*** contém links que só serão executados e exibidos quando o e-mail for aberto. Esses, p;ex., podem ser gráficos que não foram enviados com o e-mail, mas são carregados automaticamente através de um ***Hiperlink***. Como aqui pode se tratar de um gráfico nem sempre *inofensivo* , mas de uma rotina totalmente maliciosa, é sensato desativar essas referências. O texto do e-mail propriamente não é afetado por essa desativação.

Filtro da GreyList

O filtro da graylist é um método eficaz para reduzir a ocorrência de spam. Através disso, os e-mails de remetentes desconhecidos não são transferidos imediatamente através do servidor de SMTP para o destinatário do e-mail na primeira tentativa de entrega. Como os remetentes de spam normalmente não utilizam nenhuma administração de fila e seus e-mails raramente são enviados ao mesmo servidor de SMTP, a quantidade de e-mails spam pode ser significativamente reduzida.

- **Tempo de espera (minutos):** Através dessas configurações, você pode determinar quanto tempo os e-mails suspeitos devem ser bloqueados. Após a expiração desse período, o e-mail é transferido através de uma nova tentativa de envio. Quando o endereçado reagir a esse remetente, esse será retirado da greylist e inserido na whitelist. Agora a entrega desses e-mails não será mais bloqueada ou retardada.

- **Duração (dias):** Para que a whitelist dos remetentes desejados permaneça atualizada, um endereço de remetente só permanece na whitelist por um tempo determinado antes que seja novamente colocado no status Greylist. O temporizador é redefinido para cada remetente a cada novo envio de e-mail. Por exemplo, se for inserido o valor de mais de 30 dias, será possível ter os boletins informativos mensais desejados permanentemente na Whitelist.

? O filtro da graylist só pode ser selecionado quando também o **Filtro de spam** do *G Data MailSecurity* estiver ativado. Além disso, um banco de dados SQL precisa estar instalado no servidor.

Filtrar anexos

Na opção Filtrar Anexos, você tem diversas possibilidades de filtro para ***anexos de e-mail*** (= ***Attachments***). A maioria dos vírus de e-mails propagam-se através desse tipo de anexos que, em sua maioria, contêm arquivos executáveis bem ou mal escondidos. Entre eles, pode-se tratar de um arquivo EXE clássico, contendo um programa malicioso, ou também um script VB, que se esconde sob determinadas pré-condições, ou até mesmo em arquivos presumidamente seguros, de gráficos, filmes ou música. Em geral, todos os usuários devem ser extremamente cuidadosos na execução de anexos de e-mail e, em caso de dúvidas, é melhor consultar novamente o remetente do e-mail antes de executar um arquivo que não foi explicitamente solicitado. Em **Extensões de arquivos**, é possível listar as finalizações de arquivos para as quais os respetivos filtros devem ser aplicados. Assim, é possível, por exemplo, reunir todos os arquivos executáveis (como arquivos EXE e COM) em um filtro, mas também filtrar outros formatos (como MPEG, AVI. MP3, JPEG, JPG, GIF e etc,) quando esses representarem uma sobrecarga para o servidor de e-mails, devido a seu tamanho. É claro, que é possível também filtrar ***pastas compactadas*** (como ZIP, RAR ou CAB). Separe todas as extensões de arquivo de um grupo de filtragem através de um ponto e vírgula, **.exe*; **.dll* .

Em **Modo**, informe se deseja permitir, em **Extensões de arquivos**, as terminações de arquivos listadas (**Só permitir anexos informados**) ou proibir (**Filtrar anexos**).

Através da função **Filtrar também os anexos em e-mails incorporados**, você faz com que a filtragem dos tipos de anexos selecionados em **Extensões de arquivo** seja feita também em e-mails que representem, por si só, um anexo de um e-mail. Essa opção deve ser ativada em geral.

Em **Somente renomear anexos**, os anexos a serem filtrados não são excluídos automaticamente, mas apenas renomeados. Isso é bastante útil, por exemplo, em arquivos executáveis (como EXE e COM), mas também em arquivos do Microsoft Office que possivelmente possam conter scripts executáveis e macros. Ao renomear um anexo, ele não pode ser aberto inadvertidamente com um clique do mouse, mas tem que ser salvo e se necessário renomeado antes que possa ser utilizado. Quando a marcação em **Somente renomear anexos** não estiver presente, os respetivos anexos são excluídos diretamente.

Em **Sufixo**, você informa a sequência de caracteres desejada, com a qual você pretende que a extensão do arquivo seja ampliada; dessa forma, é evitada a executabilidade de um arquivo através de um simples clique (p. ex., **.exe_perigo*).

Em **Inserir aviso no texto do e-mail**, é possível informar ao destinatário do e-mail filtrado que um anexo foi excluído ou renomeado devido à regra de filtragem.

Filtro de conteúdo

Através do filtro de conteúdo, é possível bloquear de forma confortável, e-mails que contenham determinados tópicos ou textos. Para isso, em **Expressão regular**, insira as palavras-chave e expressões às quais o *G Data MailSecurity* deverá reagir e, em **Área de pesquisa**, insira em que áreas de um e-mail deverá ser procurado por essas expressões. Através do botão **Novo**, à direita do campo de entrada para **Expressão regular**, você pode confortavelmente inserir um texto que invocará a reação do filtro. Nesse processo, é possível vincular o texto da forma desejada com operadores lógicos ***E*** e ***OU***

? Se você inserir, p.ex., *Álcool* ***E*** *Drogas*, o filtro seria ativado em um e-mail que contenha, por exemplo, os termos *Álcool* e *Drogas*, mas não em um e-mail que só contenha o termo *Álcool* ou somente o termo *Drogas*. O operador lógico ***E*** tem como pré-requisito que todos os elementos vinculados com ***E*** estejam presentes e o operador ***OU***, apenas que um elemento esteja presente.

Você também pode, sem o assistente, combinar em **Expressão regular** os termos de pesquisa desejados entre si. Para isso, insira os ***termos de pesquisa*** e vincule-os aos operadores lógicos:

OU	corresponde ao ***dígito separador***	(AltGr + <)	|
E	corresponde ao ***&***	(Shift + 6)	&

Filtro de remetente

Através do filtro de remetente, é possível bloquear de forma confortável, e-mails de determinados remetentes. Para isso, basta inserir em **Endereços/Domínios** os endereços de e-mail ou os nomes dos domínios aos quais o *G Data MailSecurity* deverá reagir. Diversos registros podem ser separados através de ponto e vírgula.

? Também é possível filtrar e-mails sem remetente automaticamente.

Filtro de destinatário

Através do filtro de destinatário, é possível bloquear e-mails, confortavelmente, para determinados destinatários. Para isso, basta inserir em **Endereços/Domínios** os endereços de e-mail ou os nomes dos domínios aos quais o *G Data MailSecurity* deverá reagir. Diversos registros podem ser separados através de ponto e vírgula.

? Também é possível filtrar e-mails com o campo de destinatário em branco (ou seja, e-mails que contenham apenas Cco e/ou Cc).

Filtrar spam

Através do Filtro de spam você tem amplas possibilidades de configuração para bloquear de forma eficaz os e-mails com conteúdo ou remetentes indesejados (p.ex., remetentes de e-mail em massa). O programa verifica diversas características típicas de Spam nos e-mails. Com o auxílio das características correspondentes, é calculado um valor que espelha a possibilidade de Spam. Para isso, estão disponíveis diversas guias, nas quais todas as possibilidades de configuração são disponibilizadas e estruturadas de forma temática. O funcionamento e as possibilidades de configuração do filtro de spam são explicados detalhadamente no capítulo ***Filtro de spam***.

Filtro de IP

O filtro de IP impede o recebimento de e-mails enviados por determinados servidores. Aqui, em **Nome** e **Comentário**, insira informações sobre por que você deseja bloquear os endereços IP e depois insira cada endereço IP individual em **Não aceitar nenhum e-mail dos seguintes endereços IP**. Clique em **Adicionar** e o endereço IP inserido atualmente será aplicado à lista de endereços IP bloqueados.

Em **Modo**, você pode definir se o filtro de IP no modo Whitelist só deve permitir faixas de endereço IP ou se no modo Blacklist deve bloquear somente determinadas faixas de endereço IP>

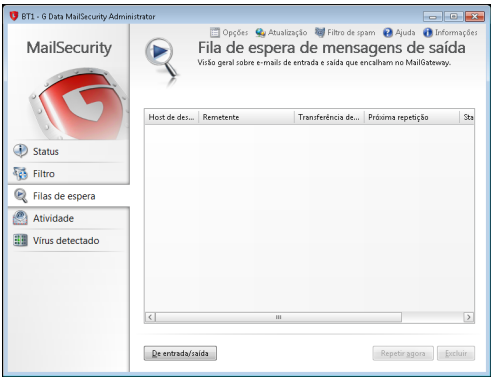
? A lista de endereços IP também pode ser exportada como arquivo txt ou importar uma lista txt correspondente com endereços IP.

Filtro de idioma

Com o Filtro de idioma, você pode definir e-mails automaticamente, em determinados idiomas, como spam. Se, por via de regra, você não tiver nenhum contato por e-mail com uma pessoa do idioma inglês, pode filtrar muitos spams através da definição do *inglês* como Idioma de spam. Selecione o idioma do qual você supõe normalmente não receber nenhum e-mail e o *G Data MailSecurity* aumenta, com isso, significativamente a avaliação de spam para esses e-mails.

Filas de espera

Na área Filas de espera, você tem permanentemente a visão geral sobre e-mails de entrada e de saída que chegam ao MailGateway e que serão verificados quanto a vírus e/ou conteúdo. Por via de regra, os e-mails são encaminhados imediatamente; através do MailGateway, sofrem um retardo mínimo e, depois, são excluídos novamente da fila de espera.



Assim que um e-mail não puder ser entregue ou ocorrerem retardos na entrega (porque o respetivo servidor não está acessível no momento) ocorre um registro correspondente na lista de espera. O *G Data MailSecurity* tenta, então, em intervalos definíveis (em ***Opções > Fila de espera)*** enviar novamente o e-mail. Uma entrega de e-mail não feita ou com retardo será, dessa forma, sempre documentada. Através do botão **De entrada/saída**, você muda da ***exibição da lista para e-mails de entrada*** para a ***exibição da lista para e-mails de saída***. Através do botão **Repetir agora**, um e-mail selecionado que não pode ser entregue, independente da definição de tempo definida para uma nova entrega em ***Opções > Fila de espera***, ser novamente entregue. Com o botão **Excluir**, você exclui para sempre um e-mail não entregável da fila.

Atividade

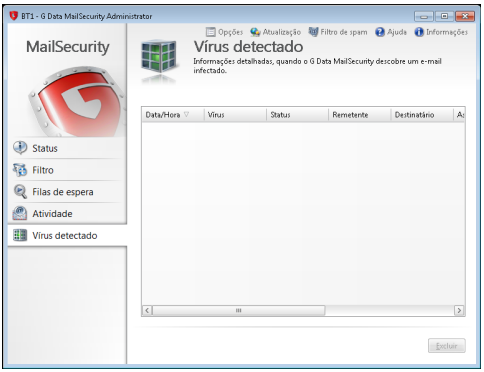
Na área Atividade, você tem, a qualquer momento, a visão geral sobre as ações executadas pelo *G Data MailSecurity*. Essas são listadas com ***Horário***, ***ID*** e ***Descrição da ação*** na lista de Atividades.

Com as barras de rolagem à direita, é possível rolar para cima ou para baixo no registro. Através do botão **Redefinir**, você exclui o registro criado até o momento e o *G Data MailSecurity* começa novamente com o registro das atividades. Com a função **Desativar rolagem de imagens**, a lista continua a ser atualizada, mas as atividades mais recentes não são exibidas diretamente em primeiro lugar. Assim, você poderá rolar pela lista de forma mais concentrada.

? Através de ***ID***, é possível atribuir claramente e-mails individuais às ações registradas. Assim, os procedimentos com a mesma ID pertencem sempre juntos (p.ex., *12345 e-mails carregados*, *12345 e-mails processados*, *12345 e-mails enviados*).

Vírus detectado

Im Virenfunde-Bereich werden sie detailliert darüber informiert, wann *G Data MailSecurity* eine infizierte Mail ermittelt hat, welche Maßnahmen dahingehend erfolgten, um welche Art von Virus es sich handelt und wer die eigentlichen Sender und Empfänger dieser betreffenden Mail sind.



Über **Löschen** entfernen Sie die jeweils ausgewählte Virenmeldung aus der Virenfunde-Liste.

Barra de menu do Administrator

Aqui você encontra as funções do software Administrator.

Opções

Na área Opções, é possível efetuar configurações abrangentes para adaptar o *G Data MailSecurity* de forma ideal às condições existentes em sua rede. Para isso, estão disponíveis diferentes Áreas de configuração, em diferentes guias as quais, com um clique na respetiva aba da guia, podem ser trazidas para primeiro plano.

De entrada (SMTP)

Nesta área, você tem a possibilidade de efetuar todas as configurações necessárias para controle de vírus de ***e-mails SMTP*** de entrada no seu servidor de e-mails.

Recebimento

Aqui é possível definir se os ***e-mails de entrada*** devem ser processados. Em geral, aqui a ***Porta 25*** é predefinida. Se devido a circunstâncias especiais não for possível usar essa ***porta padrão***, é possível, através do botão **Configurar**, definir também outras configurações para os e-mails.

Encaminhamento

Para o ***Encaminhamento*** dos e-mails de entrada a seu servidor de e-mails, desative a opção **Utilizar DNS para envio de e-mails** e, em **Encaminhar e-mails para este servidor de SMTP**, insira o servidor desejado. Informe também a **Porta** através da qual os e-mails deverão ser encaminhados ao servidor SMTP. Se diversas placas de rede estiverem disponíveis, será possível definir, através da seleção em **IP remetente**, a placa que deseja utilizar.

Proteção conta Relaying

Para impedir uma má utilização de seu servidor de e-mail, você pode e deve, em **E-mails de entrada**, definir os domínios que podem ser enviados a e-mails SMTP. Dessa forma, seu servidor não poderá ser indevidamente utilizado para o encaminhamento de e-mails SMTP a outros domínios.

> **?** ***Atenção***: Se não inserir aqui nenhum domínio, nenhum e-mail será aceito. Se todos os e-mails de todos os domínios tiverem que ser aceitos, é preciso adicionar aqui um ***.*** (asterisco ponto asterisco).

A ***proteção contra Relay*** pode ser opcionalmente realizada através de uma lista de endereços de e-mails válidos. Os e-mails para destinatários que não estão na lista não serão aceitos. Para automatizar esses endereços de e-mail, esses podem ser automática e periodicamente lidos do ActiveDirectory. Para a ***vinculação do ActiveDirectory***, é preciso pelo menos a ***.Net-Framework 1.1***.

> **?** O ***ActiveDirectory*** é um banco de dados utilizado pelo Microsoft Windows no qual informações sobre objetos (serviços, recursos ou usuários) podem ser organizadas, disponibilizadas e monitoradas pelo Administrator, centralmente na rede.

De saída (SMTP)

Nesta área, você tem a possibilidade de efetuar todas as configurações necessárias para o controle de vírus de ***e-mails SMTP*** de saída no seu servidor de e-mails.

Recebimento

Através do campo para marcação **Processar e-mails de saída**, você define se deseja controlar e-mails SMTP quanto a infecções de vírus ou não. Em **Endereços IP/Subredes dos computadores que enviam e-mails**, você pode determinar a partir de que endereços IP os e-mails a serem verificados têm origem. Quando diversos endereços IP forem utilizados, separe os endereços IP individualmente por uma vírgula. Isso é necessário para que o gateway de e-mail possa diferenciar e-mails de entrada e de saída. Em geral, a ***Porta 25*** é a definida para recebimento de e-mails de saída. Se devido a circunstâncias especiais não for possível usar essa porta padrão, é possível, através do botão **Configurar**, também definir outras configurações para e-mails.

Encaminhamento

Ative o registro **Utilizar DNS para envio de e-mails** para que os e-mails sejam enviados diretamente para os domínios de destino dos servidores de e-mail responsáveis. Se desejar enviar e-mails indiretamente através de um ***Relay*** (p.ex., um provedor), desative **Utilizar DNS para envio de e-mails** e, em **Encaminhar e-mails para este servidor de SMTP**, insira o Relay. Se diversas ***placas de rede*** estiverem disponíveis, será possível definir através da seleção em **IP remetente** a placa que deseja utilizar.

De entrada (POP3)

Nesta área, você tem a possibilidade de efetuar todas as configurações necessárias para controle de vírus de ***e-mails POP3*** de entrada, em seu servidor de e-mails.

Consultas

Em **Processar consultas POP3**, você ativa a possibilidade de, através do *G Data MailSecurity*, capturar seus ***e-mails POP3*** do respetivo servidor POP3, verificar a existência de vírus e encaminhar aos destinatários através de seu servidor de e-mail. Para isso, pode ser necessário informar a **Porta** utilizada pelo seu programa de e-mail para POP3 (normalmente a ***Porta 110***). Com a função **Evitar ultrapassar limite de tempo no programa de e-mail**, você pula o tempo que o *G Data MailSecurity* precisa para verificar e-mails e evita, assim, que o destinatário receba, ao abrir seus e-mails POP3, possivelmente uma mensagem de ***erro de tempo esgotado***, porque os dados não estão imediatamente disponíveis (mas a cada entrada de e-mail tem um retardo de alguns segundos).

? Programas de e-mail baseados em POP3 podem ser ***configurados manualmente***. Utilize, para isso, no seu programa de e-mail ***127.0.0.1*** ou servidor de seu gateway de e-mail como servidor POP3 de entrada, e escreva o nome do servidor de e-mail externo separado por dois pontos antes do nome do usuário. Ou seja, ao invés de *Servidor POP3:mail.xxx.br/nomedeusuario: Erika Modelo* escreva *Servidor POP3:127.0.0.1/nomedeusuario: mail.xxx.br:Erika Modelo*. Para executar uma configuração manual, informe-se também, no manual de instruções, de seu programa de e-mail para obter os passos necessários para configuração manual.

Captura

Em **Capturar e-mails deste servidor de POP3:** pode ser necessário informar o servidor de POP3, a partir do qual você captura os e-mails (p. ex., *pop3.provedordeemail.br*).

Filtro

Quando***e-mails POP3***, devido a uma verificação de conteúdo ou a uma infecção por vírus foram rejeitados, o remetente dessa mensagem pode ser informado automaticamente sobre isso. O **Texto de substituição para e-mails rejeitados** será: ***A mensagem foi rejeitada pelo administrador do sistema***. No entanto, o texto para essas funções de notificação podem ser editados individualmente. Para isso, também é possível utilizar espaços reservados que aplicam respetivamente os dados para o e-mail rejeitado no texto da notificação. Os seguintes ***espaços reservados*** existem à disposição no texto livremente definível para o ***Assunto*** e ***Texto do e-mail*** (definido por um sinal de percentual seguido por uma letra minúscula):

- %v ***Vírus***
- %s ***Remetente***
- %r ***Destinatário***
- %c ***Cc***
- %d ***Data***
- %u ***Assunto***
- %h ***Cabeçalho***
- %i ***IP do remetente***

Verificação de vírus

Na verificação de vírus, você tem a possibilidade de definir opções de verificação de vírus para e-mails de entrada e saída:

De entrada

Fundamentalmente, a função **Verificar a existência de vírus nos e-mails de entrada** deverá estar ativada e também deve-se observar a função que deseja utilizar **No caso de uma infecção**.

- **Somente registrar**
- **Desinfectar (se não for possível: somente registrar)**
- **Desinfectar (se não for possível: renomear)**
- **Desinfectar (se não for possível: excluir)**
- **Renomear anexos infectados**
- **Excluir anexos infectados**
- **Excluir mensagem**

Opções nas quais somente é **registrado** o vírus de entrada só devem ser utilizadas quando o seu sistema estiver de outra forma constantemente protegido contra infecções de vírus (por exemplo, com a proteção antivírus baseada em cliente/servidor do *G Data AntiVirus*). No caso de ***deteções de vírus***, existe uma grande quantidade de ***Opções de notificações***. Assim, é possível adicionar um aviso de vírus no assunto e texto do e-mail infectado e informar ao destinatário sobre um e-mail assim. Também é possível enviar um aviso sobre o vírus encontrado a determinadas pessoas, ou seja, p.ex., ao administrador do sistema ou a um funcionário responsável, que um vírus foi enviado a um endereço de e-mail em sua rede. Diversos endereços de remetente devem ser separados por um ponto e vírgula. No entanto, o texto para essas funções de notificação pode ser editado individualmente. Para isso, também é possível utilizar espaços reservados que aplicam respetivamente os dados para o e-mail rejeitado no texto da notificação. Os seguintes espaços reservados existem à disposição no texto livremente definível para o **assunto** e **Texto do e-mail** (definido por um sinal de percentual seguido por uma letra minúscula):

- %v ***Vírus***
- %s ***Remetente***
- %r ***Destinatário***
- %c ***Cc***
- %d ***Data***
- %u ***Assunto***
- %h ***Cabe•alho***
- %i ***IP do remetente***

De saída

Fundalmentalmente, a função **Verificar a existência de vírus nos e-mails de saída** e a função **Não enviar mensagem infectada** devem estar, por padrão, ativadas. Deste modo, nenhum vírus, que poderia causar danos a seus parceiros de negócios, sairá de sua rede. No caso de deteções de vírus, existe uma grande quantidade de ***Opções de notificações***. Desta forma, em **Notificar o remetente do e-mail infectado** e em **Enviar aviso de vírus às seguintes pessoas** você pode informar, p.ex., ao administrador do sistema ou a funcionários responsáveis, que um vírus deverá ser enviado de sua rede. Diversos endereços de remetente devem ser separados por um ponto e vírgula. No entanto, o texto para essas funções de notificação pode ser editado individualmente. Para isto, basta clicar no botão ... à direita. Para isso, também é possível utilizar ***espaços reservados*** que aplicam respetivamente os dados para o e-mail rejeitado no texto de notificação. Os seguintes espaços reservados existem à disposição no texto, livremente definível para o **assunto** e **Texto de e-mail** (definido por um sinal de percentual seguido por uma letra minúscula):

- %v ***Vírus***
- %s ***Remetente***
- %r ***Destinatário***
- %c ***Cc***
- %d ***Data***
- %u ***Assunto***
- %h ***Cabeçalho***
- %i ***IP do remetente***

Adicionalmente, em **Anexar relatório para e-mails de saída (não infectado)**, existe a possibilidade de anexar um relatório aos e-mails verificados pelo *G Data MailSecurity*, no qual é informado, explicitamente, que esse e-mail foi verificado pelo *G Data MailSecurity*. Naturalmente esse relatório pode ser alterado individualmente ou deixado totalmente de lado.

G Data AntiVirus Business

Após ter instalado a proteção antivírus baseada em cliente servidor, o *G Data AntiVirus* (p.ex., no escopo da solução *G Data AntiVirus Business ou G Data AntiVirus Enterprise*) poderá, colocando uma marcação em **Avisar sobre deteções de vírus no G Data AntiVirus Business**, fazer com que o software antivírus baseado em cliente/servidor, o *G Data AntiVirus*, seja informado sobre vírus encontrados no MailGateway e, dessa forma, forneça a você uma visão geral sobre a carga de vírus ou risco de sua rede.

Parâmetro da verificação

Nesta área, é possível otimizar a capacidade de reconhecimento do *G Data MailSecurity* e adaptá-la às necessidades pessoais. Em geral, através de uma redução da capacidade de reconhecimento de vírus, o desempenho do sistema completo aumenta; durante um aumento da capacidade de reconhecimento de vírus, possivelmente, isso poderá causar uma leve redução de desempenho. Aqui deve-se considerar cada caso. As seguintes funções estão disponíveis:

- **Utilizar mecanismos:**: O *G Data MailSecurity* trabalha com dois mecanismos antivírus, duas unidades operacionais de análise independentes uma da outra. Em **Utilizar mecanismos**, você define como esses cooperam entre si. Em princípio, a utilização dos dois mecanismos é a garantia para os resultados ideais da profilaxia de vírus. A utilização de um único mecanismo, ao contrário, oferece vantagens de desempenho, ou seja, ao utilizar apenas um mecanismo, o processo da análise pode ocorrer mais rapidamente.

- **Tipos de arquivos**: Em **Tipos de arquivos**, é possível definir os tipos de arquivos que o *G Data MailSecurity* deverá examinar quanto à existência de vírus. Recomendamos aqui o Reconhecimento automático de tipo, através do qual somente serão automaticamente verificados os arquivos que possam, em teoria, também conter um vírus. Quando desejar, você mesmo, definir os tipos de arquivos que deverão fazer parte de uma verificação de vírus, utilize a função **definido pelo usuário**. Um clique no botão ••• você pode abrir uma caixa de diálogo, na qual você insere os tipos de arquivos no campo de entrada superior e, através do botão **Adicionar**, aplica à lista Tipos de arquivos definidos pelo usuário Para isso, é possível trabalhar também com ***espaços reservados***, ou seja, símbolos ou cadeia de símbolos que substituem os seguintes símbolos:

  O ponto de interrogação (?) é substituto para caracteres individuais.

O asterisco (*) é substituto para sequências de caracteres inteiras.

? Para verificar todos os arquivos com a extensão de arquivo ***exe***, digite ***.exe**. Para verificar, p.ex., formatos de planilhas diferentes (p.ex.,***.xlr**, ***.xls***), basta digitar ***.xl?**. Para verificar tipos diferentes de arquivos com um nome de arquivo de início igual, digite, por exemplo, ***text*.***.

- **Heurística**: Na análise heurística, os vírus são apurados, não apenas com auxílio de bancos de dados atualizados continuamente, mas também com ajuda de características específicas típicas de vírus. Esse método é mais uma vantagem de segurança; no entanto, em raros casos, pode levar também à criação de um alarme falso.

- **Verificar pastas (compactadas)**: A verificação de ***arquivos compactados*** em pastas compactadas deverá ser ativada em geral.

- **OutbreakShield**: Com a OutbreakShield, é possível o reconhecimento e combate de pragas em e-mails em massa, antes que as assinaturas atualizadas estejam disponíveis. A OutbreakShield consulta, na Internet, sobre acúmulos especiais de e-mails suspeitos e fecha, quase em tempo real, a brecha que existe entre o começo de um e-mail em massa e seu combate através de assinaturas de vírus adaptadas especialmente. Quando desejar utilizar a ***OutbreakShield***, insira através do botão **Configurações** se utiliza um servidor proxy e, se necessário - para possibilitar a OutbreakShield um acesso contínuo - os **Dados de acesso para a conexão à Internet**. Na guia **OutbreakShield**, você pode definir o texto do e-mail que um destinatário de e-mail receberá quando um e-mail em massa destinado a ele tiver sido rejeitado.

? Como a OutbreakShield, devido a sua arquitetura própria não pode desinfectar anexos de e-mail infectados, renomeá-los ou movê-los para a quarentena, o ***Teste de substituição*** informa ao usuário que o e-mail suspeito ou infectado não foi entregue. Um aviso sobre os e-mails rejeitados através da OutbreakShield não ocorrerá, se na guia **Verificação de vírus** em **No caso de uma infecção** o item **Excluir mensagem** for selecionado. Neste caso, todos os e-mails infectados, inclusive aqueles que forem detectados exclusivamente pela OutbreakShield, são excluídos diretamente.

Fila de espera

Nesta área, é possível definir a frequência e, em intervalos, o novo envio de e-mails deverá ocorrer, que não serão encaminhados pelo MailGateway ao respetivo servidor de e-mail.

E-mails podem se encontrar na fila de espera por diversos motivos.

> **?** Em geral, os e-mails só entram na fila de espera através do *G Data MailSecurity*após a verificação de vírus.

Mensagens não entregáveis

Em **Intervalo de repetição**, informe o intervalo no qual o *G Data MailSecurity* deverá fazer uma nova tentativa de entrega. Assim, a inserção ***1, 1, 1, 4***, significa que o*G Data MailSecurity* tenta nas primeiras três horas enviar o e-mail a cada hora e, a partir daí, regularmente em intervalos de 4 horas. Em **Tempo de espera do erro**, você determina quando o envio do e-mail será interrompido totalmente e o e-mail, excluído. Você pode notificar o **remetente de mensagens na fila de espera, a cada x horas**, onde***x*** deverá ser um valor de hora inteiro. Quando você não desejar informar ao remetente sobre uma mensagem não entregável constantemente, insira aqui um ***0***.

> **?** Além disso, quando você desativa a notificação regular de remetentes de e-mails não encaminhados, o remetente será naturalmente informado, quando seu e-mail não for realmente entregue e, excluído do servidor.

Através do botão **Redefinir para os valores padrão**, é possível restaurar todas as configurações padrão na área Fila de espera. Essas configurações comprovaram-se na prática.

Limite de tamanho

O tamanho da fila de espera pode ser limitado, se desejado. Isso serve para proteção contra ***ataques de negação de serviço***. Se as restrições de tamanho forem ultrapassadas, nenhum outro e-mail será mais admitido na fila de espera.

Avançado

Na área **Avançado(a)**, você pode alterar as configurações globais do *G Data MailSecurity*.

Nome do computador

Aqui o nome do computador (***FQDN*** = ***Full Qualified Domain Name***) do servidor de e-mail pode ser alterado, se necessário.

Limite

Para limitar a quantidade de conexões de SMTP que o *G Data MailSecurity* processa simultaneamente, coloque uma marcação em **Limitar quantidade de conexões cliente de SMTP**. O *G Data MailSecurity* só permite a quantidade máxima de conexões informadas. Desta forma, é possível adaptar a filtragem de e-mail à capacidade do hardware utilizado para o MailGateway.

Mensagens do sistema

O endereço do remetente para mensagens do sistema é o endereço de e-mail que é utilizado para, p.ex., informar ao remetente e destinatário sobre e-mails infectados por vírus ou que seus e-mails se encontram na lista de espera. Os *avisos do sistema do G Data MailSecurity* independem das notificações gerais em deteções de vírus. Em um ***aviso do sistema***, normalmente trata-se de informações mais globais que possivelmente não tenham relação com um único e-mail infectado. Assim, o *G Data MailSecurity* enviaria, p.ex., um aviso do sistema, quando o controle de vírus não estivesse mais garantido. Os endereços dos destinatários para avisos do sistema podem ser idênticos aos endereços utilizados em ***De entrada/saída (SMTP, POP3)***.

Configurações

Através dos botões **Importar** e **Exportar**, é possível salvar as configurações das opções de programa também como ***arquivo XML*** e reproduzi-las quando for necessário.

Alterar senha

Aqui você pode alterar a ***senha do administrador*** que foi atribuída por você na primeira inicialização do *G Data MailSecurity*. Para isso, basta inserir a senha atual momentânea em **Senha antiga** e em **Nova senha** e **Confirmar nova senha** a nova senha. Um clique no botão **OK** executará a alteração de senha.

Registro

Na área **Registro**, você pode avaliar estatísticamente o tráfego de e-mail no seu servidor. Os resultados dessa função estatística podem ser abertos na interface do programa, clicando no botão **Estatística** na área do programa **Status**. Como alternativa, também é possivel salvar os dados em um arquivo de registro externo (registroemail.txt). Através das funções **Somente junk mails** e **Limitar quantidade de e-mails**, o tamanho desse arquivo de registro também pode ser limitado.

Atualizar

Na área Atualização, é possível efetuar configurações abrangentes para adaptar o *G Data MailSecurity* de forma ideal às condições existentes em sua rede. Aqui é possível atualizar assinaturas de vírus e dados de programa do *G Data MailSecurity* de forma manual ou automatizada.

Configurações

Aqui é possível predefinir configurações básicas para a atualização na Internet. Ao utilizar (p.ex., no escopo da *solução G Data AntiVirus Business*), paralelo ao *G Data MailSecurity*, o *G Data AntiVirus* baseado em cliente/servidor, através de **Utilizar assinaturas de vírus do G Data AntiVirus Client**, poderá ignorar o download duplo das assinaturas de vírus e obtê-las diretamente do ***G Data AntiVirus*** , porque essas já terão sido salvas no seu servidor. Através de **Executar manualmente a atualização na Internet das assinaturas de vírus**, o *G Data MailSecurity* executa, ele mesmo, esse procedimento. Através dos botão **Configurações e programação**, você é direcionado a uma área na qual poderá inserir todas as configurações necessárias para atualizações manuais e automáticas na Internet.

Dados de acesso

Em **Dados de acesso**, insira nome do usuário e senha obtidos no registro no *G Data MailSecurity*. Clique no botão **Registrar no servidor**, quando ainda não tiver se registrado no servidor *G Data*. Com a ajuda desses dados, você será reconhecido pelo servidor *G Data* e a atualização das assinaturas de vírus poderá ocorrer automaticamente.

? Se ainda não tiver feito nenhum ***registro no servidor***, poderá fazê-lo agora. Basta inserir o número de registro (- esse pode ser encontrado na contra-capa do manual do usuário -), seus dados do cliente e clicar em **Enviar**. Seus dados de acesso (nome de usuário e senha) serão exibidos imediatamente. Esses dados devem ser gravados e salvos de forma segura. Para o registro no servidor, naturalmente (-como também para a atualização na Internet das assinaturas de vírus -) é necessária uma conexão à Internet.

Programação de atualização de vírus

Através da guia **Programação da atualização de vírus**, é possível definir quando e em que Ritmo a tarefa de otimização automática deverá ocorrer. Em **Executar**, insira uma predefinição que você pode especificar em **Período**.

? Em **Diariamente**, é possível definir, com o auxílio dos dados em **Dias da semana**, que, p.ex., seu computador só executará a atualização em dias úteis ou mesmo a cada dois dias ou nos fins de semana onde ele não é utilizado para trabalhar. Para alterar registros de datas e de períodos em **Período**, selecione, com o mouse, o elemento que deseja alterar (p.ex., dia, hora, mês, ano) e utilize as teclas ou os ícones de setas à direita do campo de entrada para se movimentar de forma cronológica no respetivo elemento.

Configurações da Internet

Se utilizar um computador por trás de um ***Firewall*** ou tiver outras configurações especiais para seu acesso à Internet, utilize um ***servidor proxy***. Essas configurações só devem ser alteradas quando a atualização na Internet não funcionar. Se for necessário, fale com o provedor de Internet sobre o endereço proxy.

Os dados de acesso para a conexão à Internet (nome de usuário e senha) são especialmente importantes para a atualização programada na Internet. Sem esses dados, não poderá ocorrer nenhuma conexão automática com a Internet. Preste especial atenção para que, em suas configurações gerais da Internet (p.ex., para o programa de e-mail ou o seu navegador da Internet), a ***discagem automática*** seja permitida. Sem a discagem automática, o *G Data MailSecurity* inicia o processo de atualização na Internet, mas terá que esperar até que você confirme a Conexão à Internet com **OK**.

Através da seleção em **Região do servidor de atualizações**, você pode selecionar um servidor de atualização em sua região, para otimizar, se necessário, a transferência de dados.

Conta do usuário

Em **Conta do usuário**, informe uma conta de usuário no computador do gateway para o qual exista um acesso à Internet.

> **?** ***Atenção***: Não confunda os dados inseridos nas guias **Dados de acesso** e **Conta do usuário**.

Assinaturas de vrus

Através dos botões **Atualização de vírus** e **Atualizar status**, é possível, independente das definições feitas em Porgramação, iniciar uma atualização de vírus.

Arquivos de programa

Através do botão **Atualização do programa**, é possível atualizar os arquivos de programa do *G Data MailSecurity*, assim que ocorrerem alterações e melhorias aqui.

Filtro de spam

Através do Filtro de spam você tem amplas possibilidades de configuração para bloquear de forma eficaz os e-mails com conteúdo ou remetentes indesejados (p.ex., remetentes de e-mail em massa). O programa verifica diversas características típicas de Spam nos e-mails. Com o auxílio das características correspondentes, é calculado um valor que espelha a possibilidade de Spam. Para isso, estão disponíveis diversas guias nas quais todas as possibilidades de configuração são disponibilizadas e estruturadas de forma temática.

Filtro

Em **Nome** e **Comentário**, digite como deseja chamar o filtro e as informações adicionais que possam ser necessárias. Em **Reação**, você pode definir como o filtro de spam deve proceder com e-mails que possam conter spam. Neste processo, é possível definir três níveis que podem ser influenciados, com que nível de probabilidade o *G Data MailSecurity* utiliza para isso, já que se trata de spam no e-mail afetado.

Em **Suspeita de spam**, é regulada a manipulação de e-mails nos quais o *G Data MailSecurity* encontra elementos de spam individuais. Aqui pode, em geral, não se tratar de ***Spam***, mas, em alguns casos raros, de e-mails com boletins informativos ou e-mails conjuntos totalmente desejados pelo destinatário. Recomenda-se aqui indicar o destinatário sobre a suspeita de spam. Em **Alta probabilidade de spam**, são reunidos os e-mails que contêm as diversas características de spam e, somente em raríssimos casos, são realmente desejados pelo destinatário. Em **Altíssima probabilidade de spam**, encontram-se os e-mails que atendem a todos os critérios de um spam. Aqui, quase nunca se trata de e-mails desejados e a rejeição desse tipo de e-mail é na maioria das vezes recomendável.

? Com um ***Encaminhamento*** de tais e-mails para a***G Data***, você melhora o reconhecimento de vírus! Naturalmente essa opção também pode ser desativada.

Cada uma dessas reações com três níveis podem ser configuradas individualmente.

Assim, em **Rejeitar e-mail**, você tem a possibilidade de que o e-mail nem chegue a entrar em sua caixa de entrada. O destinatário nem chegará a receber essa mensagem. Através de **Inserir aviso de spam no assunto e texto do e-mail**, você pode informar, a um destinatário de um e-mail identificado como spam, que se trata de um spam. Através da opção **Notificar remetente da mensagem**, você pode enviar um e-mail de resposta automático ao remetente que envia e-mail reconhecido como spam, informando-lhe que seu e-mail foi reconhecido como spam. Como, justamente em spams, diversos endereços de e-mail não são utilizados apenas uma vez, você deverá pensar se deve ativar essa função. Através da opção **Encaminhar para as seguintes pessoas**, você pode encaminhar automaticamente e-mails com suspeita de spam, por exemplo, ao administrador do sistema.

Whitelist

Através da Whitelist você pode excluir determinados endereços de remetentes ou domínios, explicitamente da suspeita de spam. Para isso, basta inserir, no campo **Endereços/Domínios**, o endereço de e-mail desejado (p.ex., *gdata.de*) ou o domínio (p.ex., *gdata.de*) que deseja excluir da Suspeita de spam e o *G Data MailSecurity* não tratará e-mails desse remetente ou do domínio remetente como spam. Através do botão **Importar**, você também pode adicionar listas prontas de endereços de e-mails ou domínios na Whitelist. Os endereços e domínios deverão estar um abaixo do outro em linhas individuais na lista. Como formato, é utilizado um arquivo simples em txt que pode ser criado também com o Windows Notepad. Através do botão **Exportar**, você também pode exportar uma Whitelist como arquivo de texto.

Blacklist

Através da Blacklist, você pode colocar determinados Endereços de remetentes ou Domínios explicitamente em suspeita de spam. Para isto, basta inserir no campo **Endereços/Domínios** o endereço de e-mail desejado (p.ex., *newsletter@spamtotal.com.br*) ou o domínio (p.ex., *spamtotal.com.br*) que deseja colocar em Suspeita de spam e o *G Data MailSecurity* tratará e-mails desse remetente ou do domínio remetente em geral como **e-mails com altíssima probabilidade de spam**. Através do botão **Importar**, você também pode adicionar listas prontas de endereços de e-mails ou domínios na Blacklist. Os endereços e domínios deverão estar um abaixo do outro em linhas individuais na lista. Como formato, é utilizado um arquivo simples em txt que pode ser criado também com o Windows Notepad. Através do botão **Exportar**, você também pode exportar uma Blacklist como arquivo de texto.

Blacklists em tempo real

Na Internet existem listas negras que contêm endereços IP de servidores, através dos quais Spams são enviados. O *G Data MailSecurity* apura, através de Consultas de DNS nas ***RBLs (Realtime Blacklists)***, se o servidor que envia está listado. Caso afirmativo, aumenta a Probabilidade de spam. Em geral, deve-se utilizar aqui a configuração padrão; no entanto, é possível inserir também em ***Blacklist*** 1, 2 e 3 e endereços próprios para ***Blacklists*** da Internet.

Palavras-chave (assunto)

Através da lista de palavras-chave, você pode, com ajuda das palavras utilizadas na ***linha de assunto***, colocar e-mails em suspeita de spam. Quando pelo menos um dos termos na linha de assunto aparecer, aumenta a Probabilidade de spam. Essa lista pode ser alterada como desejado, através dos botões **Adicionar**, **Alterar** e **Excluir**. Com o botão **Importar** você também pode inserir listas de palavras-chave preparadas em sua lista. Os registros deverão estar um abaixo do outro em linhas individuais na lista. Como formato, é utilizado um arquivo simples em txt que pode ser criado também com o Windows Notepad. Através do botão **Exportar**, você também pode exportar uma lista de palavras-chave como arquivo de texto. Com a marcação em **Pesquisar somente palavras completas**, você pode definir que o *G Data MailSecurity* procure apenas por palavras inteiras na linha de assunto de um e-mail, assim, p.ex., um termo como *Casa* cairia sob suspeita de spam, enquanto um termo derivado como *Casamento*, que não significa o mesmo, permaneceria incontestado.

Palavras-chave (texto de e-mail)

Através da lista de palavras-chave, você pode, com a ajuda das palavras utilizadas no ***texto do e-mail***, colocar e-mails em suspeita de spam. Quando pelo menos um dos termos no texto do e-mail aparecer, aumenta a Probabilidade de spam. Essa lista pode ser alterada como desejado, através dos botões **Adicionar**, **Alterar** e **Excluir**.

Com o botão **Importar**, você também pode inserir listas de palavras-chave preparadas em sua lista. Os registros deverão estar um abaixo do outro em linhas individuais na lista. Como formato, é utilizado um arquivo simples em txt que pode ser criado também com o Windows Notepad.

Através do botão **Exportar**, você também pode exportar uma lista de palavras-chave como arquivo de texto. Com a marcação em **Pesquisar somente palavras completas**, você pode definir que o *G Data MailSecurity* procure apenas por palavras inteiras na linha de assunto de um e-mail, assim, p.ex., um termo como *Casa* cairia sob suspeita de spam, enquanto um termo derivado como *Casamento*, que não significa o mesmo, permaneceria incontestado.

Filtro de conteúdo

O Filtro de conteúdo é um Filtro autodidata baseado no método Bayes, que calcula, de acordo com as palavras utilizadas no Texto do e-mail uma probabilidade de spam. Esse Filtro trabalha não somente com base em listas de palavras existentes, mas aprende com cada novo e-mail recebido. Através do botão **Consultar conteúdo da tabela**, é possível solicitar as listas de palavras que o filtro de conteúdo utiliza para a classificação de um e-mail como Spam. Através do botão **Redefinir tabela** você exclui todo o conteúdo aprendido da tabela e, o filtro de conteúdo autodidata começa novamente o processo de aprendizado.

Configurações avançadas

Nesta área, é possível alterar, de forma bastante detalhada, o reconhecimento de spam do *G Data MailSecurity* e adaptar às condições de seu tráfego de e-mail. No entanto, recomenda-se em geral, utilizar as configurações padrão. Nas configurações avançadas você só deve efetuar alterações quando tiver conhecimentos sobre o assunto e souber exatamente o que faz.

Acordo de licença

A seguir estão relacionadas as condições contratuais para a utilização do *Software* ***G Data MailSecurity*** pelo usuário final (doravante também: proprietário da licença).

1. Objeto do contrato: O objeto do contrato é o *G Data Software* e a descrição do programa, gravados em uma mídia de dados ou a partir de download da Internet. Doravante chamados também de Software. A *G Data* ressalta que, de acordo com a situação tecnológica atual, não é possível criar softwares que funcionem corretamente em todos os aplicativos e combinações.

2. Escopo da utilização: A *G Data* concede o direito simples, não exclusivo e pessoal (doravante chamado também de Licença), pela duração deste contrato de utilização do software na quantidade de computadores acordada contratualmente. A utilização do software pode ocorrer na forma de uma instalação em uma unidade física (CPU), uma máquina virtual/emulada (como VMWare) ou uma instância de uma sessão de terminal. Se esse computador for também um sistema multi-usuário, esse direito de utilização vale para todos os usuários de um sistema. Como proprietário da licença, você pode transferir o software de forma física (ou seja, armazenado em uma mídia de dados) de um computador a outro, contanto que seja em algum momento, utilizado na quantidade de computadores acordada contratualmente. Não é permitida a utilização mais abrangente.

3. Restrições especiais: É proibido ao proprietário da licença alterar o software sem a prévia permissão por escrito da *G Data*.

4. Propriedade de direitos: Com a aquisição do produto você recebe apenas a propriedade da mídia de dados física, onde o software está gravado e as atualizações acordadas no escopo do suporte. Não existe vinculação da aquisição de direitos ao software. A *G Data* se reserva principalmente todos os direitos de publicação, multiplicação, processamento e utilização do software.

5. Multiplicação: O software e a respectiva documentação são protegidos pela lei de direitos autorais. É permitida a criação de uma cópia de segurança que, no entanto, não pode ser repassada a terceiros.

6. Duração do contrato: O contrato tem duração indeterminada. Esse tempo de duração não abrange o fornecimento de atualizações. O direito do proprietário da licença para utilização do software expira automaticamente e sem aviso prévio, quando esse violar uma das condições deste contrato. No encerramento do direito de utilização, o proprietário da licença é obrigado a destruir o CD-ROM original, inclusive todas as ATUALIZAÇÕES/UPGRADES, assim como a documentação escrita.

7. Restituição por danos em caso de violação do contrato: A *G Data* ressalta que, você, o proprietário da licença, é o responsável por todos os danos que possam incorrer à *G Data* devido à violações de direitos autorais e resultantes de violações das determinações deste contrato.

8. Alterações e atualizações: Respectivamente, são válidas nossas condições de serviço atuais. As condições de serviço podem ser alteradas a qualquer momento sem aviso prévio e, sem a necessidade de informação sobre os motivos.

9. Garantia e responsabilidade da *G Data*:

a) A*G Data* garante ao proprietário original da licença que, no momento da entrega do software, a eventual existência da mídia de dados (CD-ROM) onde o software foi gravado está livre de erros de execução de material, sob condições operacionais e manutenção normais.

b) Se a mídia de dados ou o download da Internet estiverem defeituosos, o comprador pode solicitar a reposição durante o tempo da garantia de 6 meses após a entrega. Para isso, a compra do software deverá ser comprovada.

c) De acordo com as razões acima citadas no item 1, a *G Data* não assume nenhuma responsabilidade pelo total funcionamento do software. Em particular, a *G Data* não assume qualquer garantia de que o software atenda às demandas e finalidades do comprador ou que funcione em compatibilidade com outros programas adquiridos. É do comprador a responsabilidade pela escolha correta e as conseqüências da utilização do software, assim como os resultados intencionados ou obtidos. O mesmo vale para a documentação escrita que acompanha o software. Se o software não estiver utilizável dentro do escopo citado no item 1, o comprador tem o direito de desfazer o contrato. A *G Data* tem o mesmo direito, quando a fabricação, dentro do escopo citado no item 1, não for possível dentro do esforço razoável.

d) A *G Data* não é responsável por danos, a não ser que o dano tenha sido causado intencionalmente ou por negligência culpável da *G Data*. A responsabilidade por negligência culpável é excluída em relação aos comerciantes. A responsabilidade de restituição máxima corresponde ao valor de compra do software.

10. Fóro: O fóro único para dirimir todos os conflitos resultantes direta ou indiretamente é, de acordo com a nossa escolha, o local da sede da *G Data*.

11. Determinações finais: Se alguma disposição deste acordo de licença for inválida, permanecerão as restantes em vigor. Como substituta da determinação inválida, valerá como acordado, uma determinação em vigor que seja mais parecida para o devido fim.

? *Copyright © 2010 G Data Software AG*

Mecanismo A: O mecanismo de verificação de vírus e os mecanismos de verificação de spyware são baseados na BitDefender technologies © 1997 -2010 BitDefender SRL.

Mecanismo B: © 2010 Alwil Software

OutbreakShield: © 2010 Commtouch Software Ltd.

[G Data MailSecurity - 26.08.2010, 17:33]

Índice

A

Acordo de licença 43
Alterar senha 36
Antes da instalação 3
AntiVirus Business 32
Área do programa do administrador 13
Arquivos de programa 38
Assinaturas de vrus 38
Atividade 24
Atualizar 36
Avançado(a) 35

B

Barra de menu do Administrator 26
Blacklist 40
Blacklists em tempo real 40

C

Captura 29
Configurações 35, 36
Configurações avançadas 42
Configurações da Internet 37
Consultas 28
Conta do usuário 38

D

Dados de acesso 37
De entrada 30
De entrada (POP3) 28
De entrada (SMTP) 26
De saída 31
De saída (SMTP) 27
Desativar referências externas 19
Desativar scripts HTML 18

E

Encaminhamento 26, 28

F

Fila de espera 34
Filas de espera 23
Filtrar anexos 20
Filtrar confirmação de leitura 18
Filtrar spam 22
Filtro 16, 29, 39
Filtro de conteúdo 21, 42
Filtro de destinatário 22
Filtro de idioma 23
Filtro de IP 22
Filtro de remetente 21
Filtro de spam 38

G

Generalidades 2

I

Instalação 7
Instalação do MailGateway em computadores separados (SMTP) 5
Instalação do MailGateway no servidor de e-mail (SMTP) 4

L

Limite 35
Limite de tamanho 34

M

MailSecurity Administrator 11
MailSecurity MailGateway 9
Mensagens do sistema 35
Mensagens não entregáveis 34

N

Nome do computador 35

O

Opções 26

Outras inicializações do programa (senha de acesso) 12

P

Palavras-chave (assunto) 41

Palavras-chave (texto de e-mail) 41

Parâmetro da verificação 32

PremiumHotline 2

Primeira inicialização do programa (atribuição de senha) 11

Programação da atualização de vírus 37

Proteção conta Relaying 27

R

Recebimento 26, 27

Registro 36

Requisitos do sistema 6

S

Status 14

V

Verificação de vírus 29

Virenfunde 25

W

Whitelist 40

Avisos